SPEED MATTERS.

THE WAYS OF THE NINJA

How it works:
A glimpse inside the many layers of MailGuards' email security protection.

mailguard


レストラン
WHEN IT COMES TO SECURING YOUR EMPIRE
AND PROTECTING YOUR TEAM, **SPEED MATTERS**.
mailguard

Many vendors fly under the radar, claiming to stop every threat, however the real question to ask is when was the threat stopped?

Don't believe the shifty charlatans whose fast hands seek to distract from reality. If an email sits in your teams' inbox for a few hours, or worse still, a few days, then the chances are that the damage is done.

All it takes is one busy and distracted employee, to click a link or download a file, and now you've been compromised. Maybe you don't even realise it yet. The enemy may be inside your walls, and you don't even know it. A bad actor may lay in wait, gathering information about your org and scanning the network, or they may act expeditiously and lock down your operating systems, or steal your database in the early stages of a ransomware attack. None of the scenarios are good.

That's why MailGuard's threat response ninjas are legendary.

Honing their techniques for several decades, since the turn of the century in 2001, they are the first to spot and block threats before they reach your inboxes. Their unique methods, though necessarily mysterious, are also evolving.

Unlike rivals, MailGuard's approach has been developed and refined entirely within its own walls, meaning that its response is nimble and agile, adapting and anticipating an adversary's advances with speed and precision.

Up to 48 hours faster than others.

mailguard

THE PRELIMINARY ROUNDS

STOPPING BAD ACTORS AT THE GATES

When an email reaches the perimeter, MailGuard checks its credentials and IP reputation to see if it may be known SPAM. At this stage, MailGuard and its ninjas have their own techniques, but they are wise enough to also check with other third parties to see what they may have seen or heard.

CHECKING FOR AUTHENTICITY

Before the new arrival is given the all-clear, MailGuard conducts validity checks to ensure that the Sender is authorised, inspecting the HELO/ EHLO, DKIM, DMARC and SPF, and ensuring that the necessary protocols are in order.

NOT TOO FAST! NOW FOR A CHALLENGE!

At the challenge stage, imposters are filtered out with grey listing checks to validate the legitimacy of the sender, recipient, and IP address.

Perimeter defences employ rate limiting and advanced mitigation techniques to repel DOS attacks.

Although many, clumsy bad actors will fail these early stages, the truth is that the most sinister and malicious are too shrewd and will likely evade early detections.

mailguard

STEPPING UP THE INTENSITY

NOW FOR THE ADVANCED LEVELS

MailGuard's strength is in the many layers that are built into its protection. Although an adversary may think they have beaten our early defences, the truth is that they are yet to truly come face to face with the best of our ninjas.

Several layers of SPAM and heuristic filters combine with proprietary anti-malware and anti-spam engines, to catch bad actors off guard. Inspecting the content in attachments, URLs and other email MIME parts recursively.

Real-time reputation algorithms, both internal and external, use multiple URL and header reputation modules and feeds to detect zero-day threats.

Our network employs proven email protection techniques, such as Bayesian analysis, fuzzy matching, static token analysis, reputation algorithms, rate limiters and more.

ANTI-VIRUS ANALYSIS

At the first of the advanced, proprietary levels of MailGuard's protection, multiple checks are conducted for known virus signatures. When a virus is found, it is marked as 'virus found, don't deliver' meaning that it is searchable in quarantine, but it is not releasable to your team.

This intelligence is instantly captured and fed back into our ninja network to assist with identifying and thwarting other attacks.

mailguard

PREPARE TO MEET A RING OF SPECIALIST NINJAS

If an email reaches it this far, it is either good, or it is among the top 1-2% of malicious and stealthy bad actors. Either way, the toughest hurdles come next.

RULES BASED ENGINES

At the highest levels of MailGuard's defences are three premium layers of protection. The first, is its rules-based engines. Scanning trillions of emails across several decades, MailGuard has amassed thousands of archives of rules and heuristic algorithms which assist in determining what a good and bad email looks like. This ancient wisdom is housed in a squad of rules-based engines, meticulously maintained, and rigorously updated by MailGuard's loyal ninja army.

The algorithms assign a threat score reflecting the propensity for evil. If an email earns a low score, it can be on its way without delay.

For more questionable emails, MailGuard will alert an admin but pass along the message for review, marking it as releasable by the destination recipient.

Where the email is more concerning, its status is elevated such that an alert is flagged and it is held in quarantine, marked for release by the admin only.

The most menacing threats are sent directly to quarantine. When MailGuard is extremely confident of the risk, it does not bother the admin with an alert. However, if for some reason in future an admin still wants to see the email, they can still search and release it at their own discretion.

mailguard

THE SUPREME LEVELS

SUPER POLICIES

Nearing the top of the tower and adversaries are confronted with the most sophisticated and complex teachings of MailGuard's ninjas. Super policies are mandatory rule sets that every email must pass before it is granted safe passage. They comprise the most ancient wisdom from MailGuard's ninjas, which is why they sit at the pinnacle of its levels.

Some of these techniques include predictive models and metas that identify rapidly varying and evolving threats derived from a known attack vector, and nested deep file analysis to analyse hidden malware or URLs that evade detection through traditional methods.

Plus, for the top 1% of extremely targeted social engineering and BEC attacks, MailGuard ninjas deploy custom built, specialized spear-phishing modules to defend against bad actors.

CUSTOM POLICIES

For those seeking to protect the most rare and precious treasures, MailGuard provides the option to configure custom policies that reflect the unique profile of your business and its assets. It's your chance to ask any final questions of someone seeking entry.

mailguard

THEY WALK AMONG US

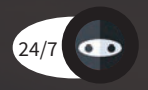
NINJA GUARDIANS INSIDE THE ROOM

If an email is good enough, we trust it and send it on its way to the end recipient inbox. The whole process is like time standing still. In milliseconds emails are processed and passed along. However, for any bad actors that do manage to slip through, the game is not yet over.

MailGuard assigns ninjas to observe emails 24/7 after they pass through the gates, and those ninjas will proactively alert the customer and others in its network and assist with intervention should anything unexpected transpire.

mailguard

MULTI-LAYERED DEFENCE



24/7 MONITORING & SUPPORT
Once an email is granted safe passage, our ninjas continue to proactively monitor the environment and intervene should any threats emerge.

1. EMAIL RECEIVED FROM THE INTERNET

2. ARRIVES AT THE PERIMETER
Check for known SPAM:
- MailGuard
- Third-party

3. AUTHENTICITY CHECKS
Conduct validity checks:
- Sender valid
- HELO/ EHLO
- Correct protocols
- SPF

4. GREYLISTING CHECKS
Challenge stage to check legitimacy:
- Sender
- Recipient
- IP

5. DOS CHECKS
Check for Denial of Service

6. ANTI-VIRUS ANALYSIS
Check for known signature viruses:
- Multiple checks

7. RULES BASED ENGINES
Algorithms attribute a threat/ risk propensity score to determine the propensity for evil.

8. SUPER POLICIES
A proprietary rule set that is mandatory for all customers.

9. CUSTOM POLICIES
Tailored policies that are configurable to the risk profile of the business.

10. TRUSTED EMAILS DELIVERED
Trusted emails are delivered to the final destination email server.

mailguard

If sophisticated, email-borne cyber attacks are a concern for your business, **don't wait until it's too late.**

Talk to our team of local experts.

1300 304 430

expert@mailguard.com.au

mailguard